UNITED STATES DEPARTMENT OF AGRICULTURE
FOOD SAFETY AND INSPECTION SERVICE
WASHINGTON, DC

# FSIS DIRECTIVE	5420.3, Revision 3	9/14/06

HOMELAND SECURITY THREAT CONDITION RESPONSE – MONITORING AND SURVEILLANCE OF PRODUCTS IN COMMERCE

I. PURPOSE

A. This directive describes the procedures that personnel of the Compliance and Investigations Division (CID), Office of Program Evaluation, Enforcement and Review (OPEER), Food Safety and Inspection Service (FSIS), will follow when the Department of Homeland Security declares a threat condition Yellow, Orange, or Red.

B. This directive also provides:

- food defense surveillance procedures to aid in the detection of possible vulnerabilities to meat, poultry, and egg products in commerce;

- a mechanism to document the findings from food defense surveillance procedures; and

- the method for communicating elevated threat conditions within FSIS, and how CID personnel will respond to elevated threat conditions.

C. If there is an actual terrorist attack on a facility that handles product in commerce, OPEER personnel will take immediate measures to ensure the safety of any affected FSIS personnel and notify appropriate law enforcement officials and the Assistant Administrator of OPEER.

II. CANCELLATION

FSIS Directive 5420.3, Revision 2, dated 1/26/05

DISTRIBUTION: Inspection Offices; T/A Inspectors; TRA; TSC; Import Offices

OPI: OPPED

III. REASON FOR REISSUANCE

FSIS is reissuing this directive in its entirety to:

- include specific tasks that OPEER personnel are to conduct during food defense surveillance activities at or above a threat condition "Elevated" (Yellow) level; and

- provide instructions for communicating the results of those surveillance activities to appropriate levels in FSIS.

IV. REFERENCES

9 CFR part 300 to end
FSIS Directive 5420.1, Revision 3, Homeland Security Threat Condition Response – Food Defense Verification Procedures
FSIS Directive 5500.2, Non-Routine Incident Response

V. BACKGROUND

In 2002, the White House Office of Homeland Security established a Homeland Security Advisory System based on color. This System provides a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities and to the American people. A declaration of a Threat Condition Elevated (Yellow) by the Department of Homeland Security indicates that there is an elevated risk of terrorist attacks. A declaration of a Threat Condition High (Orange) indicates that there is a high risk of terrorist attacks. A declaration of a Threat Condition Severe (Red) reflects a severe risk of terrorist attacks. While the threat may or may not involve the nation's food supply, it is imperative that inspection program personnel take certain immediate actions during such threat conditions to ensure the safety of meat, poultry, and egg products. Given what is required in responding to a credible threat of a terrorist attack, program personnel must clearly understand their roles and what will be required of them to respond properly to that threat.

VI. NOTIFICATION

A. In the event of a declaration of any threat condition:

- Elevated (Yellow), when there is a significant risk of terrorist attacks,
- High (Orange), when there is a high risk of terrorist attacks, or
- Severe (Red) when there is a severe risk of terrorist attacks,

by the Department of Homeland Security, FSIS' Office of Food Defense and Emergency Response (OFDER) will inform the FSIS Administrator and the FSIS Management Council. OFDER will issue an e-mail letter to all employees notifying them of the heightened threat condition.

B. OFDER will communicate the downgrading of a threat condition to CID personnel through the senior executive leadership in OPEER.

VI. FOOD DEFENSE SURVEILLANCE

1. FSIS Investigators will conduct the food defense surveillance activities listed in paragraph VII below at threat condition "Yellow" or higher and will use the intranet-based "Share Point" application for food defense surveillance procedures to document the findings.

2. Performing food defense surveillance procedures identifies and mitigates, to the maximum extent possible, potential vulnerabilities that could lead to the deliberate contamination of meat, poultry, or egg products in commerce.

3. CID supervisors and managers, as well as other OPEER and OFDER managers, will have access to the data entered by Investigators, in addition to having access to summary reports of the data in the "Share Point" application. Access by CID supervisors and managers will also allow them to amend or revise a Non-Routine Incident Report.

VII. SPECIFIC THREAT CONDITION ACTIVITIES

There are no specific enhanced food defense surveillance activities during threat condition "Low" (Green) and "Guarded" (Blue). However, OPEER managers will use these times during lower threat conditions to update and validate existing emergency information and procedures from lessons learned.

A. Threat Condition Elevated (Yellow), High (Orange), or Severe (Red) with no specific threat to the food and agriculture sector

FSIS Investigators will conduct the following food defense surveillance activities:

1. Food Defense Plan – determine whether the facility (e.g., warehouse, distribution center, import house) has the following:

a. a written food defense plan that consists of specific standard operating procedures for preventing intentional product tampering and for responding to threats or actual incidents of intentional product tampering; and

b. emergency contact information available.

2. Outside Security – determine whether the facility:

a. has secured the area during non-operating hours; and

b. has outdoor lighting for detection of unusual activities conducted under the cover of darkness.

3. General Inside Security – determine whether the facility:

a. maintains an active surveillance system;

b. restricts access to production areas (in businesses such as restaurants, catering facilities), and to storage, staging, loading and transfer areas, to authorized personnel;

c. regularly schedules monitoring by authorized firm personnel or maintains a surveillance system of secluded areas where it holds products or materials;

d. protects the water supply from unauthorized access; and,

e. protects the building environmental systems (e.g., electricity, ventilation, etc., or natural resources such as water and natural gas) from unauthorized access.

4. Shipping and Receiving – determine whether:

a. access to the loading dock or receiving area is restricted to authorized personnel; and,

b. there is a verification process for incoming shipments of products or materials.

If Investigators observe product adulteration or misbranding at any time, they are to immediately follow the established policy described in FSIS Directive 8410.1, Detention and Seizure. When FSIS has reason to believe that meat, poultry, or egg products in commerce are adulterated or misbranded, or otherwise in violation of the Federal Meat Inspection Act, Sec. 402, (21 U.S.C. 672); Poultry Products Inspection Act, Sec 19, (21 U.S.C. 467a); or the Egg Products Inspection Act, Sec 19, (21 U.S.C. 1048), FSIS may detain such products. Program Investigators will follow procedures defined in FSIS Directive 5500.2, Non-Routine Incident Response, when they determine that there is reason to believe that product adulteration was intentional.

CID headquarters will notify its personnel when the threat level changes from yellow to orange or red with no specific threat to the food and agriculture sector, in addition to the e-mail notification from OFDER. The CID Regional Offices, upon this notification by CID headquarters of the threat level, will:

a. ensure on-call procedures and updated facility personnel contact information are in place and ready for activation: and

b. direct Investigators to inform the businesses visited during the course of their duties of the current threat level.

B. Threat Condition High (Orange) with a specific threat to the food and agriculture sector.

1. CID headquarters managers and CID Regional Offices will be placed in a 24/7 on-call status. The CID Regional Offices, upon notification by CID headquarters of the threat level, will:

a. place CID field supervisors in a 24/7 on-call status; and

b. immediately direct CID field personnel to conduct and document in "Share Point" the following food defense surveillance activities, in addition to those listed in paragraph VII above, in warehouses, distribution centers, import houses, and transporters (e.g., particularly in trucks and, to a lesser extent, in rail cars and planes):

i. coordinate activity at ports of entry with Office of International Affairs (OIA) personnel;

ii. collect samples of products as needed; and

iii. increase food defense surveillance activities as directed by OPEER management.

2. CID field personnel will conduct these food defense surveillance activities to determine whether the facilities have:

a. meat, poultry, and egg products from approved foreign sources;

b. a means to prevent tampering with products;

c. appropriate measures in place to ensure that contractors (e.g., construction or maintenance personnel) are authorized and properly identified when they have access to meat, poultry, and egg products;

d. a process to observe all incoming products and to verify the shipping documents;

e. adequate use and storage procedures for any hazardous materials in the facility to preclude product adulteration; and,

f. an employee identification system and a process to notify management when unfamiliar people appear in unassigned areas.

C. Threat Condition Severe (Red) with a specific threat to the food and agriculture sector.

All CID headquarters and CID Regional Office personnel will be placed in a 24/7 on-call status. The CID Regional Office, upon notification of the threat level, will:

a. take all actions outlined under threat condition High (Orange) involving a specific threat to the food and agriculture sector;

b. place all field personnel in a 24/7 on-call status; and

c. carry out any additional activities as directed by CID headquarters, OPEER management, emergency response issuances, or incident command.

All questions on this directive are to be directed through supervisory channels.

Assistant Administrator
Office of Policy, Program, and Employee Development